Federal Energy Regulatory Commission
Washington, D.C. 20426
December 22, 2021

Re: FOIA No. FY19-30
Thirty Ninth Determination Letter
Release

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.clom

Dear Mr. Mabee:

This is a response to your correspondence received in January 2019, in which you requested information pursuant to the Freedom of Information Act (FOIA),[1] and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108 (2019).

By letter dated December 17, 2021, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC13-1, along with the names of three (3) relevant UREs inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC13-1.

With respect to the remaining identities of UREs contained in RC13-1, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the

[1] 5 U.S.C. § 552 (2018).

[2] This docket involves multiple UREs and notification of the FOIA request as well as the Notice of Intent to Release were only sent to the UREs for whom FERC initially determined that disclosure of identities may be appropriate.

following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow the Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-related information is contained in the Notices of Penalty (NOP); whether mitigation is complete; the content of the public and non-public versions of the NOP; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public NOP. An application of these factors will dictate whether a particular FOIA exemption, including 7(F) and/or Exemption 3, is appropriate. *See Garcia v. U.S. DOJ,* 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger.") (citation and internal quotations omitted).

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC13-1 will not be disclosed.

On November 18, 2019, you filed suit in the U.S. District Court for the District of Columbia asserting claims in connection with this FOIA request. *See Mabee v. Fed. Energy Reg. Comm'n.,* Civil Action No. 19-3448 (KBJ) (D.D.C.). Because this FOIA request is currently in litigation, this letter does not contain information regarding administrative appeal of the response to the FOIA request. For any further assistance or to discuss any aspect of your request, you may contact Assistant United States Attorney T. Anthony Quinn by email at Tony.Quinn2@usdoj.gov, by phone at (202) 252-7558, or

by mail at United States Attorney's Office – Civil Division, U.S. Department of Justice, 555 Fourth Street, N.W., Washington, DC 20530.

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2021.12.22 14:10:14 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

Peter Sorenson, Esq.
Counsel for Mr. Mabee
petesorenson@gmail.com

James M. McGrane
Senior Counsel
North American Electric Reliability Corporation
1325 G Street N.W. Suite 600
Washington, D.C. 20005
James.McGrane@nerc.net

Filed Date: 10/31/2012
Document Accession #: 20121031-5394

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC13-1

Public Service Electric & Gas Company (PSE&G) - .pdf page 27

October 31, 2012

CPS Energy (CPS)-.pdf page 30

Ms. Kimberly Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Pend Oreille County Public Utility District No. 1 (POPD) - .pdf page 31

Re: NERC FFT Informational Filing
FERC Docket No. RC13-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find, Fix, Track and Report[1] (FFT Spreadsheet) in Attachment A regarding 44 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

This FFT resolves 82 possible violations[5] of 22 Reliability Standards that posed a minimal risk to the reliability of the bulk power system (BPS). In all cases, the possible violations contained in this FFT have been found and fixed, so they are now described as "remediated issues." A certification of completion of the mitigation activities has been submitted by the respective Registered Entities.

As discussed below, this FFT includes 82 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Corresponding NERC Registry ID Numbers for each Registered Entity are identified in Attachment A.
[3] Attachment A is an Excel spreadsheet.
[4] *See* 18 C.F.R § 39.7(c)(2).
[5] For purposes of this document, each matter is described as a "possible violation," regardless of its procedural posture.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

enforcement processes for occurrences that posed a minimal risk to the BPS.[6] Resolution of these minimal risk possible violations in this reporting format is an appropriate disposition of these matters, and will help NERC and the Regional Entities focus on the more serious violations of the mandatory and enforceable NERC Reliability Standards.

Statement of Findings Underlying the FFT

The descriptions of the remediated issues and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval by NERC Enforcement staff, under delegated authority from the NERC Board of Trustees Compliance Committee (NERC BOTCC), of the findings reflected in Attachment A. In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), each Reliability Standard at issue in this FFT is identified in Attachment A.

Text of the Reliability Standards at issue in the FFT may be found on NERC's website at http://www.nerc.com/page.php?cid=2|20. For each respective remediated issue, the Reliability Standard Requirement at issue is listed in Attachment A.

Status of Mitigation[7]

As noted above and reflected in Attachment A, the possible violations identified in Attachment A have been mitigated. The respective Registered Entity has submitted a certification of completion of the mitigation activities to the Regional Entity. These mitigation activities are subject to verification by the Regional Entity via an audit, a spot check, a random sampling, a request for information, or otherwise. These activities are described in Attachment A for each respective possible violation.

[6] *See North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 (2012) ("March 15, 2012 CEI Order"); *see also North American Electric Reliability Standards Development and NERC and Regional Entity Enforcement*, 132 FERC ¶ 61,217 at P.218 (2010)(encouraging streamlined administrative processes aligned with the significance of the subject violations).
[7] *See* 18 C.F.R § 39.7(d)(7).

Statement Describing the Resolution[8]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order and the August 27, 2010 Guidance Order,[9] NERC Enforcement staff under delegated authority from the NERC BOTCC, approved the FFT based upon its findings and determinations, as well as its review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the remediated issues.

Notice of Completion of Enforcement Action

In accordance with section 5.10 of the CMEP, and the Commission's March 15, 2012 CEI Order, provided that the Commission has not issued a notice of review of a specific matter included in this filing, notice is hereby provided that, sixty-one days after the date of this filing, enforcement action is complete with respect to all remediated issues included herein and any related data holds are released only as to that particular remediated issue.

Pursuant to the Commission order referenced above, both the Commission and NERC retain the discretion to review a remediated issue after the above referenced sixty-day period if it finds that FFT treatment was obtained based on a material misrepresentation of the facts underlying the FFT matter. Moreover, to the extent that it is subsequently determined that the mitigation activities described herein were not completed, the failure to remediate the issue will be treated as a continuing possible violation of a Reliability Standard requirement that is not eligible for FFT treatment.

Request for Confidential Treatment of Certain Attachments

Certain portions of Attachment A include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain

[8] *See* 18 C.F.R § 39.7(d)(4).
[9] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010).

Reliability Standard possible violations and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the information in the attached documents is deemed "confidential" by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be included as Part of this FFT Informational Filing

The attachments to be included as part of this FFT Informational Filing are the following documents and material:

a) FFT Spreadsheet, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

A Form of Notice Suitable for Publication[10]

A copy of a notice suitable for publication is included in Attachment C.

[10] *See* 18 C.F.R § 39.7(d)(6).

Document Accession #: 20121031-5394 Filed Date: 10/31/2012

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this FFT:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net

Conclusion

Handling these remediated issues in a streamlined process will help NERC, the Regional Entities, Registered Entities, and the Commission focus on improving reliability and holding Registered Entities accountable for the more serious violations of the mandatory and enforceable NERC Reliability Standards. Accordingly, NERC respectfully submits this FFT as an informational filing.

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
charles.berardesco@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
rebecca.michael@nerc.net

cc: Entities listed in Attachment B

NERC

Attachment a

Find, Fix, Track and Report Spreadsheet (Included in a Separate Document)

Document Accession #: 20121031-5394 Filed Date: 10/31/2012

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR OCTOBER 2012
FIND, FIX, TRACK AND REPORT (FFT) INFORMATIONAL FILING

FOR MRO:

Daniel P. Skaar*
President
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1731
dp.skaar@midwestreliability.org

Sara E. Patrick*
Director of Regulatory Affairs and Enforcement
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1708
se.patrick@midwestreliability.org

FOR NPCC:

Walter Cintron*
Manager, Compliance Enforcement
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
wcintron@npcc.org

Edward A. Schwerdt*
President and Chief Executive Officer
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
eschwerdt@npcc.org

Stanley E. Kopman*
Assistant Vice President of Compliance
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
skopman@npcc.org

FOR RFC:

Robert K. Wargo*
Director of Analytics & Enforcement
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
bob.wargo@rfirst.org

L. Jason Blake*
General Counsel
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
jason.blake@rfirst.org

Megan E. Gambrel*
Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
megan.gambrel@rfirst.org

Michael D. Austin*
Managing Enforcement Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
mike.austin@rfirst.org

FOR SERC:

John R. Twitchell*
VP and Chief Program Officer
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8205
(704) 357-7914 – facsimile
jtwitchell@serc1.org

Marisa A. Sifontes*
General Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7775
(704) 357-7914 – facsimile
msifontes@serc1.org

Maggie A. Sallah*
Senior Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7778
(704) 357-7914 – facsimile
msallah@serc1.org

James M. McGrane*
Legal Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7787
(704) 357-7914 – facsimile
jmcgrane@serc1.org

Andrea B. Koch*
Manager, Compliance Enforcement and Mitigation
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8219
(704) 357-7914 – facsimile
akoch@serc1.org

FOR SPP RE:

Ron Ciesiel*
General Manager
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223
(501) 614-3265
(501) 482-2025 – facsimile
rciesiel.re@spp.org

Joe Gertsch*
Manager of Enforcement
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223
(501) 688-1672
(501) 482-2025 – facsimile
jgertsch.re@spp.org

Peggy Lewandoski*
Paralegal & SPP RE File Clerk
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223
(501) 482-2057
(501) 482-2025 – facsimile
spprefileclerk@spp.org

FOR TEXAS RE:

Susan Vincent*
General Counsel
Texas Reliability Entity, Inc.
805 Las Cimas Parkway
Suite 200
Austin, TX 78746
(512) 583-4922
(512) 233-2233 – facsimile
susan.vincent@texasre.org

Rashida Caraway*
Manager, Compliance Enforcement
Texas Reliability Entity, Inc.
805 Las Cimas Parkway
Suite 200
Austin, TX 78746
(512) 583-4977
(512) 233-2233 – facsimile
rashida.caraway@texasre.org

FOR WECC:

Mark Maher*
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(360) 713-9598
(801) 582-3918 – facsimile
Mark@wecc.biz

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6855
(801) 883-6894 – facsimile
CWhite@wecc.biz

Ruben Arredondo*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7674
(801) 883-6894 – facsimile
RArredondo@wecc.biz

Christopher Luras*
Director of Enforcement
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6887
(801) 883-6894 – facsimile
CLuras@wecc.biz

Sandy Mooy*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7658
(801) 883-6894 – facsimile
SMooy@wecc.biz

Document Accession #: 20121031-5394 Filed Date: 10/31/2012

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. RC13-___-000

NOTICE OF FILING
October 31, 2012

Take notice that on October 31, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding forty-four (44) Registered Entities in seven (7) Regional Entity footprints.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211, 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken, but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. Such notices, motions, or protests must be filed on or before the comment date. On or before the comment date, it is not necessary to serve motions to intervene or protests on persons other than the Applicant.

The Commission encourages electronic submission of protests and interventions in lieu of paper using the "eFiling" link at http://www.ferc.gov. Persons unable to file electronically should submit an original and 14 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street, N.E., Washington, D.C. 20426.

This filing is accessible on-line at http://www.ferc.gov, using the "eLibrary" link and is available for review in the Commission's Public Reference Room in Washington, D.C. There is an "eSubscription" link on the web site that enables subscribers to receive email notification when a document is added to a subscribed docket(s). For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	National Grid USA	NCR11171	NPCC2012009728	PRC-005-1a	R2; R2.1	On January 27, 2012, National Grid USA, as a Distribution Provider and Transmission Owner, self-reported an issue with PRC-005-1a R2.1. National Grid USA failed to complete annual communication testing of a three-terminal transmission line within the intervals defined in its Protection System maintenance and testing program because of scheduling problems. The annual communication testing was scheduled to be completed by December 31, 2011 and was actually completed on January 27, 2012.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because National Grid USA did perform a non-intrusive inspection of its equipment associated with the transmission line. The risk during the pendency of the issue was mitigated by National Grid USA's inspection and testing on as much of its communications facilities as was possible without participation of the other entities. The system redundancies, system monitoring, and system alarming also mitigated the interim reliability risk. The transmission line is designed with two fully independent high-speed relaying systems for line protection. Neither system experienced any alarm conditions during the period of the issue. System tests were completed 27 days past the expected date with no problems found. NPCC considered the compliance history of affiliates and the fact that they do not share compliance documents or responsibilities, in determining that FFT treatment was warranted.	To mitigate this issue, National Grid USA adjusted its testing schedule so that the annual communication channel test for the transmission line will be scheduled earlier during each calendar year. The earlier scheduled test date will reduce the probability that the test will not be completed during the time period required by the National Grid USA procedure. The 2012 annual telecommunications testing is now scheduled for the beginning of October with a proposed rain date. Confirmation between all interconnected entities for the annual testing have been completed.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Altona Windpark, LLC	NCR10366	NPCC2012010199	CIP-001-1	R1	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Altona Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R1 for failing to have a procedure for recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. This condition existed since August 14, 2009, when Noble Altona Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Altona Windpark, LLC did not have a procedure for recognizing sabotage and making operating personnel aware of sabotage events on its facilities and multi-sabotage affecting larger portions of the Interconnection, its parent company, Noble Environmental Power did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Altona Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Furthermore, Noble Altona Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 97.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Altona Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Altona Windpark, LLC	NCR10366	NPCC2012010200	CIP-001-1	R2	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Altona Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R2 for failing to have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection. This condition existed since August 14, 2009, when Noble Altona Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Altona Windpark, LLC did not have a procedure for recognizing sabotage or communicating information concerning sabotage events to appropriate parties in the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Altona Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Noble Altona Windpark, LLC also had an emergency phone list, including the Federal Bureau of Investigation, for making notification of emergency events. Furthermore, Noble Altona Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 97.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Altona Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, including the communication of information concerning sabotage events to appropriate parties in the Interconnection; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Altona Windpark, LLC	NCR10366	NPCC2012010201	CIP-001-1	R3	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Altona Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R3 for failing to have guidelines for its operating personnel for sabotage events, including all the personnel to contact for reporting disturbance due to sabotage events. This condition existed since August 14, 2009, when Noble Altona Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Altona Windpark, LLC did not have sabotage response guidelines for reporting disturbances due to sabotage and therefore could not provide such guidelines to its operating personnel, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Altona Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage, as well as response guidelines for reporting those emergencies. Furthermore, Noble Altona Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 97.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Altona Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, provided its operating personnel with sabotage response guidelines and included personnel to contact for reporting sabotage event disturbances; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Bliss Windpark, LLC	NCR10271	NPCC2012010206	CIP-001-1	R1	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Bliss Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R1 for failing to have a procedure for recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. This condition existed since October 15, 2008, when Noble Bliss Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Bliss Windpark, LLC did not have a procedure for recognizing sabotage and making operating personnel aware of sabotage events on its facilities and multi-sabotage affecting larger portions of the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Bliss Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Furthermore, Noble Bliss Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 100.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Bliss Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Bliss Windpark, LLC	NCR10271	NPCC2012010207	CIP-001-1	R2	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Bliss Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R2 for failing to have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection. This condition existed since October 15, 2008, when Noble Bliss Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Bliss Windpark, LLC did not have a procedure for recognizing sabotage or communicating information concerning sabotage events to appropriate parties in the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Bliss Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Noble Bliss Windpark, LLC also had an emergency phone list, including the Federal Bureau of Investigation, for making notification of emergency events. Furthermore, Noble Bliss Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 100.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Bliss Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, including the communication of information concerning sabotage events to appropriate parties in the Interconnection; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Bliss Windpark, LLC	NCR10271	NPCC2012010208	CIP-001-1	R3	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Bliss Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R3 for failing to have guidelines for its operating personnel for sabotage events, including all the personnel to contact for reporting disturbance due to sabotage events. This condition existed since October 15, 2008, when Noble Bliss Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Bliss Windpark, LLC did not have sabotage response guidelines for reporting disturbances due to sabotage and therefore could not provide such guidelines to its operating personnel, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Bliss Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage, as well as response guidelines for reporting those emergencies. Furthermore, Noble Bliss Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 100.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Bliss Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, provided its operating personnel with sabotage response guidelines and included personnel to contact for reporting sabotage event disturbances; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Chateaugay Windpark, LLC	NCR10367	NPCC2012010213	CIP-001-1	R1	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Chateaugay Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R1 for failing to have a procedure for recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. This condition existed since August 14, 2009, when Noble Chateaugay Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Chateaugay Windpark, LLC did not have a procedure for recognizing sabotage and making operating personnel aware of sabotage events on its facilities and multi-sabotage affecting larger portions of the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Chateaugay Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Furthermore, Noble Chateaugay Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 106.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Chateaugay Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Chateaugay Windpark, LLC	NCR10367	NPCC2012010214	CIP-001-1	R2	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Chateaugay Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R2 for failing to have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection. This condition existed since August 14, 2009, when Noble Chateaugay Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Chateaugay Windpark, LLC did not have a procedure for recognizing sabotage or communicating information concerning sabotage events to appropriate parties in the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Chateaugay Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Noble Chateaugay Windpark, LLC also had an emergency phone list, including the Federal Bureau of Investigation, for making notification of emergency events. Furthermore, Noble Chateaugay Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 106.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Chateaugay Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, including the communication of information concerning sabotage events to appropriate parties in the Interconnection; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Chateaugay Windpark, LLC	NCR10367	NPCC2012010215	CIP-001-1	R3	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Chateaugay Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R3 for failing to have guidelines for its operating personnel for sabotage events, including all the personnel to contact for reporting disturbance due to sabotage events. This condition existed since August 14, 2009, when Noble Chateaugay Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Chateaugay Windpark, LLC did not have sabotage response guidelines for reporting disturbances due to sabotage and therefore could not provide such guidelines to its operating personnel, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Chateaugay Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage, as well as response guidelines for reporting those emergencies. Furthermore, Noble Chateaugay Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 106.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Chateaugay Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, provided its operating personnel with sabotage response guidelines and included personnel to contact for reporting sabotage event disturbances; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Clinton Windpark, LLC	NCR10272	NPCC2012010192	CIP-001-1	R1	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Clinton Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R1 for failing to have a procedure for recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. This condition existed since October 15, 2008, when Noble Clinton Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Clinton Windpark, LLC did not have a procedure for recognizing sabotage and making operating personnel aware of sabotage events on its facilities and multi-sabotage affecting larger portions of the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Clinton Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Furthermore, Noble Clinton Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 100.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Clinton Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Clinton Windpark, LLC	NCR10272	NPCC2012010193	CIP-001-1	R2	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Clinton Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R2 for failing to have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection. This condition existed since October 15, 2008, when Noble Clinton Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Clinton Windpark, LLC did not have a procedure for recognizing sabotage or communicating information concerning sabotage events to appropriate parties in the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Clinton Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Noble Clinton Windpark, LLC also had an emergency phone list, including the Federal Bureau of Investigation, for making notification of emergency events. Furthermore, Noble Clinton Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 100.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Clinton Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, including the communication of information concerning sabotage events to appropriate parties in the Interconnection; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Clinton Windpark, LLC	NCR10272	NPCC2012010194	CIP-001-1	R3	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Clinton Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R3 for failing to have guidelines for its operating personnel for sabotage events, including all the personnel to contact for reporting disturbance due to sabotage events. This condition existed since October 15, 2008, when Noble Clinton Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Clinton Windpark, LLC did not have sabotage response guidelines for reporting disturbances due to sabotage and therefore could not provide such guidelines to its operating personnel, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Clinton Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage, as well as response guidelines for reporting those emergencies. Furthermore, Noble Clinton Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 100.5 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Clinton Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, provided its operating personnel with sabotage response guidelines and included personnel to contact for reporting sabotage event disturbances; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Ellenburg Windpark, LLC	NCR10273	NPCC2012010220	CIP-001-1	R1	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Ellenburg Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R1 for failing to have a procedure for recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. This condition existed since October 15, 2008, when Noble Ellenburg Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Ellenburg Windpark, LLC did not have a procedure for recognizing sabotage and making operating personnel aware of sabotage events on its facilities and multi-sabotage affecting larger portions of the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Ellenburg Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Furthermore, Noble Ellenburg Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 81 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Ellenburg Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Ellenburg Windpark, LLC	NCR10273	NPCC2012010221	CIP-001-1	R2	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Ellenburg Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R2 for failing to have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection. This condition existed since October 15, 2008, when Noble Ellenburg Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Ellenburg Windpark, LLC did not have a procedure for recognizing sabotage or communicating information concerning sabotage events to appropriate parties in the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Ellenburg Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Noble Ellenburg Windpark, LLC also had an emergency phone list, including the Federal Bureau of Investigation, for making notification of emergency events. Furthermore, Noble Ellenburg Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 81 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Ellenburg Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, including the communication of information concerning sabotage events to appropriate parties in the Interconnection; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Ellenburg Windpark, LLC	NCR10273	NPCC2012010222	CIP-001-1	R3	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Ellenburg Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R3 for failing to have guidelines for its operating personnel for sabotage events, including all the personnel to contact for reporting disturbance due to sabotage events. This condition existed since October 15, 2008, when Noble Ellenburg Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Ellenburg Windpark, LLC did not have sabotage response guidelines for reporting disturbances due to sabotage and therefore could not provide such guidelines to its operating personnel, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Ellenburg Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage, as well a response guidelines for reporting those emergencies. Furthermore, Noble Ellenburg Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 81 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Ellenburg Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, provided its operating personnel with sabotage response guidelines and included personnel to contact for reporting sabotage event disturbances; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Wethersfield Windpark, LLC	NCR10368	NPCC2012010706	CIP-001-1	R1	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Wethersfield Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R1 for failing to have a procedure for recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. This condition existed since August 14, 2009, when Noble Wethersfield Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Wethersfield Windpark, LLC did not have a procedure for recognizing sabotage and making operating personnel aware of sabotage events on its facilities and multi-sabotage affecting larger portions of the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Wethersfield Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Furthermore, Noble Wethersfield Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 126 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Wethersfield Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Wethersfield Windpark, LLC	NCR10368	NPCC2012010228	CIP-001-1	R2	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Wethersfield Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R2 for failing to have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection. This condition existed since August 14, 2009, when Noble Wethersfield Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Wethersfield Windpark, LLC did not have a procedure for recognizing sabotage or communicating information concerning sabotage events to appropriate parties in the Interconnection, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Wethersfield Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage. Noble Wethersfield Windpark, LLC also had an emergency phone list, including the Federal Bureau of Investigation, for making notification of emergency events. Furthermore, Noble Wethersfield Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 126 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the Interconnection.	To mitigate the issue, Noble Wethersfield Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, including the communication of information concerning sabotage events to appropriate parties in the Interconnection; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Noble Wethersfield Windpark, LLC	NCR10368	NPCC2012010229	CIP-001-1	R3	During an off-site Compliance Audit ending on July 1, 2011, NPCC determined that Noble Wethersfield Windpark, LLC, as a Generator Operator, had an issue with CIP-001-1 R3 for failing to have guidelines for its operating personnel for sabotage events, including all the personnel to contact for reporting disturbance due to sabotage events. This condition existed since August 14, 2009, when Noble Wethersfield Windpark, LLC was registered on the NERC Compliance Registry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Noble Wethersfield Windpark, LLC did not have sabotage response guidelines for reporting disturbances due to sabotage and therefore could not provide such guidelines to its operating personnel, its parent company, Noble Environmental Power, did have an emergency response policy, utilized by its affiliated wind generation units (including Noble Wethersfield Windpark, LLC), that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid and that could occur as a result of sabotage, as well as response guidelines for reporting those emergencies. Furthermore, Noble Wethersfield Windpark, LLC is a wind-powered variable energy facility with a maximum capacity of 126 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the interconnection.	To mitigate the issue, Noble Wethersfield Windpark, LLC: 1. Implemented a written procedure for recognizing and making operating personnel aware of sabotage events, provided its operating personnel with sabotage response guidelines and included personnel to contact for reporting sabotage event disturbances; and 2. Provided sabotage training to site personnel. NPCC has verified completion of the mitigation activities.
Reliability*First* Corporation (Reliability*First*)	Fowler Ridge II Wind Farm LLC (Fowler Ridge II)	NCR03040	RFC2012010792	VAR-002-1.1b	R2	During a Compliance Audit, conducted from May 2, 2011 to May 17, 2011, ReliabilityFirst discovered that Fowler Ridge III, as a Generator Operator, had an issue with VAR-002-1.1b R2. Fowler Ridge, Fowler Ridge II and Fowler Ridge III (collectively, Fowler Ridge Companies) are affiliates that share metering at their point of interconnection. Subsequently, on May 2, 2011, Fowler Ridge II, as a Generator Operator, self-reported this issue with VAR-002-1.1b R2 based on the same facts discovered at the Fowler Ridge III Compliance Audit. Fowler Ridge III is required to maintain Reactive Power output as defined by its Transmission Operator (TOP). American Electric Power provides criteria for Fowler Ridge III's Reactive Power output in a power factor schedule within its Interconnection Service Agreement with the Fowler Ridge Companies. Fowler Ridge III's power factor schedule requires a power factor of 1.00 plus or minus 5.0% at its Dequine 345 kV substation, also the point of interconnection with American Electric Power. On numerous occasions Fowler Ridge III failed to maintain the power factor within the required range. During the Compliance Audit, Fowler Ridge III provided an outdated power factor schedule that contained a narrower range. After the Compliance Audit, Fowler Ridge III provided the correct schedule, which resulted in fewer instances of Fowler Ridge III failing to maintain Reactive Power output. Additionally, because Fowler Ridge III shares metering with Fowler Ridge and Fowler Ridge II at its point of interconnection, it cannot determine which of the excursions were attributable to which affiliate.	Reliability*First* determined that this posed a minimal risk to the reliability of the bulk power system (BPS) because although the Fowler Ridge Companies failed to maintain their power factor schedule, the Fowler Ridge Companies maintained voltage at all relevant times and have not been directed to modify voltage since their initial operation. Additionally, all of the power factor excursions occurred when the output of the Fowler Ridge Companies was at or less than 25 percent of nameplate capacity, when the wind farms have limited dynamic reactive control, and would not have been considered excursions under the Fowler Ridge Companies' power factor scheduled updated in July 2012. Moreover, as small, wind-powered generating facilities, the Fowler Ridge Wind Farm Complex's generation output is variable by nature and not coincident with peak load. As a result of these inherent characteristics and its limited ability to produce dispatchable power, the Fowler Ridge Wind Farm Complex has a relative lesser impact on the BPS.	The Fowler Ridge Companies took action to mitigate the issue. The Fowler Ridge Companies worked with their TOP to revise their power factor schedule to better reflect design criteria, operating conditions, and characteristics inherent to the limited dynamic reactive control capabilities of wind farms. On July 20, 2012, American Electric Power issued a new power factor schedule that addresses these factors by applying the schedule to the Fowler Ridge Companies only when the units are online and generating greater than or equal to 25 percent of the total wind farm nameplate capacity.
Reliability*First* Corporation (Reliability*First*)	Fowler Ridge III Wind Farm LLC (Fowler Ridge III)	NCR10308	RFC201100996	VAR-002-1.1b	R2	During a Compliance Audit, conducted from May 2, 2011 to May 17, 2011, ReliabilityFirst discovered that Fowler Ridge III, as a Generator Operator, had an issue with VAR-002-1.1b R2. Fowler Ridge, Fowler Ridge II and Fowler Ridge III (collectively, Fowler Ridge Companies) are affiliates that share metering at their point of interconnection. Fowler Ridge III is required to maintain Reactive Power output as defined by its Transmission Operator (TOP). American Electric Power provides criteria for Fowler Ridge III's Reactive Power output in a power factor schedule within its Interconnection Service Agreement with the Fowler Ridge Companies. Fowler Ridge III's power factor schedule requires a power factor of 1.00 plus or minus 5.0% at its Dequine 345 kV substation, also the point of interconnection with American Electric Power. On numerous occasions Fowler Ridge III failed to maintain the power factor within the required range. During the Compliance Audit, Fowler Ridge III provided an outdated power factor schedule that contained a narrower range. After the Compliance Audit, Fowler Ridge III provided the correct schedule, which resulted in fewer instances of Fowler Ridge III failing to maintain Reactive Power output. Additionally, because Fowler Ridge III shares metering with Fowler Ridge and Fowler Ridge II at its point of interconnection, it cannot determine which of the excursions were attributable to which affiliate.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because although the Fowler Ridge Companies failed to maintain their power factor schedule, the Fowler Ridge Companies maintained voltage at all relevant times and have not been directed to modify voltage since their initial operation. Additionally, all of the power factor excursions occurred when the output of the Fowler Ridge Companies was at or less than 25 percent of nameplate capacity, when the wind farms have limited dynamic reactive control, and would not have been considered excursions under the Fowler Ridge Companies' power factor scheduled updated in July 2012. Moreover, as small, wind-powered generating facilities, the Fowler Ridge Wind Farm Complex's generation output is variable by nature and not coincident with peak load. As a result of these inherent characteristics and its limited ability to produce dispatchable power, the Fowler Ridge Wind Farm Complex has a relative lesser impact on the BPS.	The Fowler Ridge Companies took action to mitigate the issue. The Fowler Ridge Companies worked with their TOP to revise their power factor schedule to better reflect design criteria, operating conditions, and characteristics inherent to the limited dynamic reactive control capabilities of wind farms. On July 20, 2012, American Electric Power issued a new power factor schedule that addresses these factors by applying the schedule to the Fowler Ridge Companies only when the units are online and generating greater than or equal to 25 percent of the total wind farm nameplate capacity.
Reliability*First* Corporation (Reliability*First*)	Fowler Ridge Wind Farm LLC (Fowler Ridge)	NCR10307	RFC2012010791	VAR-002-1.1b	R2	During a Compliance Audit, conducted from May 2, 2011 to May 17, 2011, ReliabilityFirst discovered that Fowler Ridge III, as a Generator Operator, had an issue with VAR-002-1.1b R2. Fowler Ridge, Fowler Ridge II and Fowler Ridge III (collectively, Fowler Ridge Companies) are affiliates that share metering at their point of interconnection. Subsequently, on May 2, 2011, Fowler Ridge, as a Generator Operator, self-reported this issue with VAR-002-1.1b R2 based on the same facts discovered at the Fowler Ridge III Compliance Audit. Fowler Ridge III is required to maintain Reactive Power output as defined by its Transmission Operator (TOP). American Electric Power provides criteria for Fowler Ridge III's Reactive Power output in a power factor schedule within its Interconnection Service Agreement with the Fowler Ridge Companies. Fowler Ridge III's power factor schedule requires a power factor of 1.00 plus or minus 5.0% at its Dequine 345 kV substation, also the point of interconnection with American Electric Power. On numerous occasions Fowler Ridge III failed to maintain the power factor within the required range. During the Compliance Audit, Fowler Ridge III provided an outdated power factor schedule that contained a narrower range. After the Compliance Audit, Fowler Ridge III provided the correct schedule, which resulted in fewer instances of Fowler Ridge III failing to maintain Reactive Power output. Additionally, because Fowler Ridge III shares metering with Fowler Ridge and Fowler Ridge II at its point of interconnection, it cannot determine which of the excursions were attributable to which affiliate.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because although the Fowler Ridge Companies failed to maintain their power factor schedule, the Fowler Ridge Companies maintained voltage at all relevant times and have not been directed to modify voltage since their initial operation. Additionally, all of the power factor excursions occurred when the output of the Fowler Ridge Companies was at or less than 25 percent of nameplate capacity, when the wind farms have limited dynamic reactive control, and would not have been considered excursions under the Fowler Ridge Companies' power factor scheduled updated in July 2012. Moreover, as small, wind-powered generating facilities, the Fowler Ridge Wind Farm Complex's generation output is variable by nature and not coincident with peak load. As a result of these inherent characteristics and its limited ability to produce dispatchable power, the Fowler Ridge Wind Farm Complex has a relative lesser impact on the BPS.	The Fowler Ridge Companies took action to mitigate the issue. The Fowler Ridge Companies worked with their TOP to revise their power factor schedule to better reflect design criteria, operating conditions, and characteristics inherent to the limited dynamic reactive control capabilities of wind farms. On July 20, 2012, American Electric Power issued a new power factor schedule that addresses these factors by applying the schedule to the Fowler Ridge Companies only when the units are online and generating greater than or equal to 25 percent of the total wind farm nameplate capacity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
ReliabilityFirst Corporation (ReliabilityFirst)	Indianapolis Power & Light Company (IPL)	NCR00798	RFC2012010447	EOP-001-0	R6	On May 31, 2012, IPL, as a Balancing Authority (BA) and Transmission Operator, self-reported an issue with EOP-001-0 R6 to ReliabilityFirst. IPL has a Coordinated Functional Registration (CFR) with Midwest Independent Transmission System Operator (MISO) whereby MISO performs certain of IPL's BA functions. The individual responsible for the *Transmission System Emergency Operating Plan* that IPL developed pursuant to EOP-001-0 R3.2 mistakenly believed that MISO would complete the annual review of this plan pursuant to the CFR. As a result of this mistake, IPL did not perform an annual review of this plan in 2011. In fact, IPL was required to annually review the *Transmission System Emergency Operating Plan,* as required by EOP-001-0 R6.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because the only substantial updates to the *Transmission System Emergency Operating Plan* during the pendency of the issue were organizational name changes and updated distribution lists. In addition, many of the elements of the plan existed within other emergency plans that IPL had properly reviewed and updated annually.	IPL committed to take certain actions to mitigate the issue. IPL reviewed and updated the *Transmission System Emergency Operating Plan.* In addition, IPL incorporated an electronic reminder to automatically send an alert to the individual responsible for updating the emergency plan.
ReliabilityFirst Corporation (ReliabilityFirst)	InterPower/ Ahlcon Partners, Limited Partnership [GOP] (InterPower)	NCR02604	RFC2012009867	VAR-002-1.1b	R2	From November 7, 2011 through November 12, 2011, ReliabilityFirst conducted a Compliance Audit of InterPower (Audit). During the Audit, ReliabilityFirst discovered that InterPower, as a Generator Operator, had an issue with VAR-002-1.1b R2. InterPower's voltage schedule for its 110 MW Colver generating plant is 116.5 kV plus or minus 1.5% for normal and light load conditions and 117.5 kV plus or minus 1.5% for heavy load conditions or when requested. On May 18, 2011, May 22, 2011, and September 14, 2011, during light load conditions, InterPower exceeded its voltage schedule by less than 1% of the voltage schedule.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system. The risk to the BPS was mitigated by the following factors. InterPower attested that its Transmission Operator (TOP) relies on the Colver generating plant as a reactive power resource in addition to maintaining the generator voltage schedule. InterPower's TOP has provided direction to InterPower regarding the Colver plant's generator voltage or reactive power output throughout both a voltage schedule and the ongoing expectation that InterPower operate the plant as a reactive power resource that results in slightly positive MVARs at the interconnection point. When operating the plant in this manner, system load variations may occasionally cause slight deviations from the voltage schedule. While InterPower did not seek or receive an exemption from its voltage schedule during these events, InterPower believed it was carrying out the directive of its TOP. In addition, the automatic voltage regulator was in automatic voltage control mode during the voltage excursions, and InterPower did not have a voltage excursion greater than 1%.	InterPower committed to take certain actions to mitigate the issue. InterPower worked with Corporate NERC Compliance to identify additional measures to better control the voltage output within the voltage schedule parameters while still responding to the expectation of slightly positive MVARs at the interconnection point as expected by the TOP. Specifically, InterPower posted the voltage schedule in the control room, conducted operator meetings on the use of the voltage schedule, and created voltage alarms in the control system to alert the operator of voltage deviations. In addition, between December 2011 and March 2012, InterPower's Corporate NERC Compliance staff initiated and completed a comprehensive VAR-002 R2 compliance review of its entire NERC-registered generation fleet. This was a review of 23 facilities located across five NERC regions and yielded no additional VAR-002 R2 compliance issues.
ReliabilityFirst Corporation (ReliabilityFirst)	Northern Indiana Public Service Company (NIPSCO)	NCR02611	RFC2012010014	EOP-008-0	R1	From December 6, 2011 through December 13, 2011, ReliabilityFirst conducted a Compliance Audit of NIPSCO (Audit). During the Audit, ReliabilityFirst discovered that NIPSCO, as a Balancing Authority and Transmission Operator, had an issue with EOP-008-0 R1. ReliabilityFirst determined that NIPSCO's Operations and Cyber Recovery Plan (Plan) to continue reliability operations if their control center becomes inoperable was not sufficient to demonstrate compliance with EOP-008-0, R1.5 and R1.6. Specifically, in its Plan NIPSCO states, "[t]he Electric Transmission Department is to coordinate tests, at least annually, of this recovery plan. Operating personnel shall review and undergo training at least annually on the procedures and responsibilities contained within this plan." ReliabilityFirst determined, based on these two sentences, that the Plan lacked procedures and responsibilities for conducting periodic tests, at least annually, or for providing annual training pursuant to EOP-008-0 R1.5 and R1.6.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because it is a documentation issue. Although NIPSCO did not adequately document EOP-008-0 R1.5 and R1.6 in its Plan, NIPSCO conducted annual testing demonstrating the viability of the Plan and provided training to its personnel as part of its annual testing to ensure operating personnel were able to successfully implement the Plan. NIPSCO ensures the viability of the Plan and that operating personnel are able to implement the Plan by performing annual testing in which NIPSCO personnel successfully engage the backup control center and take over the operation of the energy management system to operate in real-time. NIPSCO utilizes various departmental documents, procedures, and checklists which tests the viability of the Plan during this annual exercise. The responsibilities for conducting periodic tests to ensure viability of the Plan are reflected in the various departmental documents, procedures, and checklists. Therefore, although NIPSCO's Plan did not adequately address EOP-008-0 R1.5 and R1.6, NIPSCO was conducting an annual exercise during which NIPSCO successfully engaged its backup control center. This annual exercise included procedures and responsibilities that ensured the viability of the Plan and NIPSCO operating personnel's ability to implement the Plan.	NIPSCO created a document on the procedures and responsibilities for conducting periodic tests and included procedures and responsibilities for providing annual training that reflects the practices it is already implementing.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
ReliabilityFirst Corporation (ReliabilityFirst)	PPL Holtwood, L.L.C. (PPL Holtwood)	NCR00886	RFC2011001215	VAR-002-1.1b	R1	On November 7, 2011, PPL Holtwood, as a Generator Operator, self-reported to ReliabilityFirst an issue with VAR-002-1.1b R1 and R3. On October 3, 2011, after flooding caused by a recent tropical storm, PPL Holtwood operations and maintenance personnel were working to locate and clear electrical grounds on the 125 volt direct current and 125 volt alternating current electrical systems. This work included checking the motor-operated valves on the plant drainage pumps in the operating tunnel and opening a circuit breaker and de-energizing a cabinet that contains plant control equipment. The ongoing work caused PPL Holtwood's Unit 5 to reduce megawatt output from full output, which is approximately 10 MW. In response to a unit alarm alerting the hydro plant control operator to switch Unit 5's turbine governor to manual mode, the hydro plant control operator switched Unit 5's automatic voltage regulator (AVR) from automatic to manual voltage control mode. In response to the megawatt output reduction, the hydro plant control operator attempted to open the gates that control the flow of water supply for a hydroelectric generating unit, but could not do so until the governor was placed into hand control mode. At the time the hydro plant control operator placed the governor switch in hand control mode, the operator also placed the AVR in manual. However, the hydro plant control operator failed to notify the Transmission Operator (TOP) that the Unit 5 AVR was not in automatic voltage control mode, as required by VAR-002-1.1b R1. In addition, the hydro plant control operator failed to notify the TOP within 30 minutes of the status change on the AVR, as required by VAR-002-1.1b R3. The afternoon shift hydro plant control operator noticed that the Unit 5 AVR was operating in manual mode and switched the AVR back to automatic voltage control mode. At this time, PPL Holtwood notified the TOP of the status change on the Unit 5 AVR.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because during the time period of the issue, six generating units at PPL Holtwood were operating with their AVRs in automatic voltage control mode and were therefore able to provide any required voltage or reactive support. In addition, PPL Holtwood maintained its voltage schedule during the time period of the issue. A PJM letter confirming that the PPL Generation entities, which includes PPL Holtwood, "have not caused any reliability concerns on the PJM Bulk Electric System with respect to their operating within the PJM voltage criteria outlined in PJM Manual 14D" provides verification that no adverse system events occurred during the 6.5 hours that the AVR was in manual mode. Finally, the issue implicated one of the generating units, which had a ten MW generating capacity.	PPL Holtwood completed the following mitigating activities: 1) installed visible reminders at each voltage regulator control switch to prompt the operators to contact the individuals who notify the TOP when the AVR status changes; 2) implemented an additional level of monitoring by connecting the AVR status indication to the generation management system; 3) reviewed procedures related to excitation system operation in the various governor modes with the appropriate individuals; and 4) reviewed the NERC Reliability Standard Requirements with the appropriate individuals.
ReliabilityFirst Corporation (ReliabilityFirst)	PPL Holtwood, LLC (PPL Holtwood)	NCR00886	RFC2011001216	VAR-002-1.1b	R3	On November 7, 2011, PPL Holtwood, as a Generator Operator, self-reported to ReliabilityFirst an issue with VAR-002-1.1b R1 and R3. On October 3, 2011, after flooding caused by a recent tropical storm, PPL Holtwood operations and maintenance personnel were working to locate and clear electrical grounds on the 125 volt direct current and 125 volt alternating current electrical systems. This work included checking the motor-operated valves on the plant drainage pumps in the operating tunnel and opening a circuit breaker and de-energizing a cabinet that contains plant control equipment. The ongoing work caused PPL Holtwood's Unit 5 to reduce megawatt output from full output, which is approximately 10 MW. In response to a unit alarm alerting the hydro plant control operator to switch Unit 5's turbine governor to manual mode, the hydro plant control operator switched Unit 5's automatic voltage regulator (AVR) from automatic to manual voltage control mode. In response to the megawatt output reduction, the hydro plant control operator attempted to open the gates that control the flow of water supply for a hydroelectric generating unit, but could not do so until the governor was placed into hand control mode. At the time the hydro plant control operator placed the governor switch in hand control mode, the operator also placed the AVR in manual. However, the hydro plant control operator failed to notify the Transmission Operator (TOP) that the Unit 5 AVR was not in automatic voltage control mode, as required by VAR-002-1.1b R1. In addition, the hydro plant control operator failed to notify the TOP within 30 minutes of the status change on the AVR, as required by VAR-002-1.1b R3. The afternoon shift hydro plant control operator noticed that the Unit 5 AVR was operating in manual mode and switched the AVR back to automatic voltage control mode. At this time, PPL Holtwood notified the TOP of the status change on the Unit 5 AVR.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because during the time period of the issue, six generating units at PPL Holtwood were operating with their AVRs in automatic voltage control mode and were therefore able to provide any required voltage or reactive support. In addition, PPL Holtwood maintained its voltage schedule during the time period of the issue. A PJM letter confirming that the PPL Generation entities, which includes PPL Holtwood, "have not caused any reliability concerns on the PJM Bulk Electric System with respect to their operating within the PJM voltage criteria outlined in PJM Manual 14D" provides verification that no adverse system events occurred during the 6.5 hours that the AVR was in manual mode. Finally, the issue implicated one of the generating units, which had a ten MW generating capacity.	PPL Holtwood completed the following mitigating activities: 1) installed visible reminders at each voltage regulator control switch to prompt the operators to contact the individuals who notify the TOP when the AVR status changes; 2) implemented an additional level of monitoring by connecting the AVR status indication to the generation management system; 3) reviewed procedures related to excitation system operation in the various governor modes with the appropriate individuals; and 4) reviewed the NERC Reliability Standard Requirements with the appropriate individuals.
ReliabilityFirst Corporation (ReliabilityFirst)	Whitewater Operating Services, LLC (Whitewater)	NCR10156	RFC2012010609	VAR-002-1.1b	R3	On June 25, 2012, Whitewater, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3 to ReliabilityFirst. On June 10, 2012, Whitewater started its steam turbine generator and synchronized it to the grid at 6:24 a.m. Approximately 14 minutes later, Whitewater noticed the steam turbine generator's automatic voltage regulator (AVR) was not controlling voltage automatically, at which time Whitewater's shift operator began to control voltage manually. Whitewater notified its Transmission Operator (TOP), American Transmission Company, of the status change on its AVR 36 minutes after its steam turbine generator was synchronized to the grid.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because the issue was caused by an isolated incident; the Whitewater operator closing a breaker earlier in the generator's startup procedures than required. The Whitewater operator began manual voltage control within 14 minutes of synchronization to the grid, and Whitewater notified its TOP within 36 minutes of the status change on its AVR.	On June 10, 2012, 36 minutes after the status change on its AVR, Whitewater notified its TOP. By virtue of this notification, Whitewater mitigated this issue.
ReliabilityFirst Corporation (ReliabilityFirst)	Whitewater Operating Services, LLC (Whitewater)	NCR10156	RFC2012010677	VAR-002-1.1b	R1	On June 25, 2012, Whitewater, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3 to ReliabilityFirst. ReliabilityFirst determined that the reported facts also constituted an issue with VAR-002-1.1b R1. On June 10, 2012, Whitewater started its steam turbine generator and synchronized it to the grid at 6:24 a.m. Approximately 14 minutes later, Whitewater noticed the steam turbine generator's automatic voltage regulator (AVR) was not controlling voltage automatically, at which time Whitewater's shift operator began to control voltage manually. Whitewater notified its Transmission Operator (TOP), American Transmission Company, of the status change on its AVR 36 minutes after its steam turbine generator was synchronized to the grid.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because the issue was caused by an isolated incident; the Whitewater operator closing a breaker earlier in the generator's startup procedures than required. The Whitewater operator began manual voltage control within 14 minutes of synchronization to the grid, and Whitewater notified its TOP within 36 minutes of the status change on its AVR.	On June 10, 2012, 36 minutes after the status change on its AVR, Whitewater notified its TOP. By virtue of this notification, Whitewater mitigated this issue.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Electric Energy, Inc. (EEI)	NCR01230	SERC2011007386	BAL-002-0	R4	On June 6, 2011, EEI, as a Balancing Authority (BA), self-reported an issue with BAL-002-0 R4.2, stating that it experienced a Reportable Disturbance in the form of a unit trip that resulted in a drop in the Area Control Error (ACE) greater than 80% of the most severe single contingency. Following that event, EEI did not return ACE to zero within 15 minutes as required by BAL-002-0 R4.2. On June 5, 2011, EEI's Unit 3 tripped offline, resulting in a drop in the ACE greater than 80% of EEI's largest single contingency. EEI's largest single contingency is 167 MW. At the time of the event, Unit 3 was at 170 MW (158 MW net) and ACE was at +3 MW. ACE dropped to -163 MW immediately following the trip. The EEI systems operator contacted Midwest Independent Transmission System Operator, Inc. (MISO) to arrange a 170 MW coordinated adjustment to the interchange schedule. However, the systems supervisor was slow in entering the 10-minute ramped adjustment in supervisory control and data acquisition (SCADA) which caused EEI to exceed the 15 minute limit to restore ACE. EEI returned ACE to zero within 17 minutes of the start of the Reportable Disturbance.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. EEI was two minutes late in returning ACE to zero after the start of the Reportable Disturbance; and 2. MISO had sufficient reserves to cover the Disturbance Control Standard event. Although EEI has violated this Standard previously, the instant remediated issue nonetheless does not represent recurring conduct by EEI. The prior violation occurred in 2008, when EEI failed to achieve a Disturbance Control Standard (DCS) event average recovery of 100% for the third quarter of 2008. Following the prior violation, EEI reviewed the event with EEI system operators to reemphasize the BAL-002-0 requirements, reviewed EEI's Reserve Policy, and also reviewed appropriate actions including options to utilize during a DCS event. In addition to the actions described in the Mitigation Plan, EEI also applied the appropriate Contingency Reserve Adjustment Factor (CRAF) of 101.75% relative to their single largest contingency of 167 MW, which increased EEI's Contingency Reserve requirement from 167 MW to 170 MW to help prevent recurrence of a similar violation. The prior violation was considered and distinguished because it occurred approximately three years before the current issue, indicating this was not a problem with recurring conduct by EEI.	SERC verified that EEI has completed the following actions: 1. Conducted a performance improvement discussion with the employees involved in the event; 2. Communicated with the systems operator the importance of being able to curtail interchange schedules quickly in the event of a unit trip; 3. Increased EEI's Contingency Reserve obligation from 167 MW to 189 MW of curtailable interchange schedules; 4. Revised the job task in EEI's Quality Training Database for balancing the loss of a major generation resource by curtailing interchange; and 5. Re-trained each systems supervisor using the revised job task from the database and issued a memo re-emphasizing EEI's Reserve Policy.
SERC Reliability Corporation (SERC)	Electric Energy, Inc. (EEI)	NCR01230	SERC2011007534	PRC-005-1	R2	On June 28, 2011, EEI, as a Generator Owner (GO) and Transmission Owner (TO), self-reported an issue with PRC-005-1 R2, stating that it did not have evidence that all relays were maintained and tested within the defined intervals of its Protection System maintenance and testing program. SERC reviewed a spreadsheet prepared by EEI that included each of its Protection System devices and the defined maintenance and testing intervals, the most recent test date, and the previous test date for each device. SERC verified the defined intervals based on a review of EEI's Protection System maintenance and testing procedures. Based on this review, SERC determined that EEI tested 16 out of 176 protective relays (9.1%) and five out of six batteries (83.3%) outside of their defined intervals. In total, EEI tested 21 out of 556 Protection System devices (3.8%) outside of their defined intervals.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. EEI's batteries are alarmed with direct current (DC) ground, loss of power, and voltage alarms, which would alert EEI personnel to possible problems and prompt them to investigate; 2. Although EEI conducted the five-year battery load test three to six years outside of the defined interval, it still tested and maintained the batteries according to the monthly, quarterly and annual requirements; and 3. Although the relays were tested two to five years late, EEI's subsequent testing of the relays was successful and found no problems, suggesting that the relays likely would have performed as intended if called upon to do so.	SERC verified that EEI has completed the following actions: 1. Tested the 16 identified protective relays and documented the test results; 2. Revised its internal procedures such that the system engineer responsible for protective relays will review EEI's list of NERC auditable relays on an annual basis and verify that the list is complete and accurate and that all of the relays on the list are scheduled for regular testing within the defined intervals in the Protection System maintenance and testing procedure. The system engineer is also required to work with the maintenance planning department to ensure that work orders are automatically generating for the testing of each NERC auditable relay and that procedures exist so that testing can be performed. The revised procedure also requires the maintenance supervisor responsible for protective relays to conduct a quarterly review of all work orders related to NERC auditable maintenance and verify that the work orders are issued and executed timely. A list of open NERC auditable work orders is generated and distributed to the group supervisor electrical maintenance and the system engineer; and 3. Revised its internal procedures such that the system engineer responsible for batteries is required to work with the maintenance planning department to ensure that work orders are automatically generating for the testing of each battery set and that procedures exist so that testing can be performed. The revised procedure also requires the maintenance supervisor responsible for batteries to conduct a quarterly review of all work orders related to NERC auditable maintenance and verify that the work orders are issued and executed within the required timeframe. A list of open NERC auditable work orders is generated and distributed to the group supervisor electrical maintenance and the system engineer.
SERC Reliability Corporation (SERC)	Electric Energy, Inc. (EEI)	NCR01230	SERC2011007876	FAC-008-1	R1	On August 10, 2011, the SERC audit team reported an issue with FAC-008-1 R1, stating that EEI, as a Transmission Owner (TO), did not include series and shunt compensation devices within the scope of its Facility Ratings Methodology (FRM). SERC reviewed EEI's 2010 version of its FRM and confirmed the audit team's finding that the FRM did not include series and shunt compensation devices for the TO function. SERC also determined that the FRM failed to address series and shunt compensation devices for the Generator Owner function. SERC reviewed all versions of EEI's FRM back to June 18, 2007 and confirmed that series and shunt compensation devices were not addressed in any of them. EEI owns a bus tie series reactor and developed a Facility Rating for the series reactor using its nameplate rating.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. EEI considered series and shunt compensation devices despite its failure to document it. EEI owns a bus tie series reactor, which is a series compensation device. EEI developed and used a Facility Rating for the series reactor using its nameplate rating; and 2. After documenting series and shunt compensation devices in its FRM, EEI's Rating for the series reactor did not change and the most limiting device did not change.	SERC verified that EEI revised its FRM to include a section detailing its rating methodology for series and shunt compensation devices.

Attachment A-2

October 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO2012010722	CIP-007-3	R6; R6.2	MRO_URE1 self-reported noncompliance with CIP-007-3 R6 because it did not have automatic alerting enabled on several Critical Cyber Assets (CCAs) for 129 days. More specifically, two physical servers and nine virtual servers were deployed with improper configuration; therefore automatic alerts for detected cybersecurity incidents would not have been sent, as required by R6.2. When implementing new devices, MRO_URE1 executes a compliance readiness checklist. The checklist contains each configuration task for setting up controls used for achieving compliance. The checklists for these devices were completed successfully. However, the script used to configure alerting had a typo, so the alerts were not being received. The misconfiguration was identified and corrected after 129 days.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices were protected by several layers of cybersecurity controls including: anti-virus/anti-malware software; up-to-date security patches; and authentication controls such as complex passwords. The CCAs were also located in an Electronic Security Perimeter and a Physical Security Perimeter as required. Finally, logs covering the entire period were available, and a review of the logs confirmed that no cybersecurity incidents had occurred.	Upon discovery, MRO_URE1 immediately corrected the alerting and monitoring functionality. Additionally, logs were reviewed to verify that no events occurred during the lapse in alerting. Lastly, the compliance readiness process has been updated to include a test verifying the functionality of alerting at the time of implementation. This should result in the immediate detection of any configuration errors before any lapse in alerting occurs. MRO verified that MRO_URE1 completed its mitigating activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO2012010723	CIP-004-3	R4	MRO_URE1 self-reported noncompliance with CIP-004-3 R4 because it failed to maintain its list of individuals authorized for unescorted physical and/or cyber access to Critical Cyber Assets (CCAs). Specifically, one employee was granted cyber access accidentally outside of the standard process, so the access was not properly documented in the list. The issue was identified during a quarterly review process and was mitigated within 55 days, outside the 7 calendar days of any change of personnel with access, as required by R4.1. The quarterly review encompassed all individuals with CCA access.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the access granted to the employee was read-only, and was appropriate for the employee's role. Additionally, the employee in question was already approved for other CCA access and had a proper personnel risk assessment and cybersecurity training as required by the Standards.	Upon discovery, the access approval was documented in the NERC CIP access management tool, which recorded the business need as determined by the designated approver and synched up the authorized and configured access lists. Because controls are already implemented for access management, the processes for obtaining access were not changed. Instead, additional reminders were sent to management via letter regarding following established procedures, and a quick reference card was distributed to all personnel responsible for NERC CIP access configuration. MRO verified that MRO_URE1 completed its mitigating activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2012010669	CIP-005-1	R1; R1.6	NPCC_URE1 self-reported an issue with CIP-005-1 R1.6. Specifically, two servers that are Cyber Assets used to support systems within the Electronic Security Perimeter (ESP) were connected to a switch using a virtual LAN that was not documented as a non-critical Cyber Asset.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because BPS operations would not be impacted if the systems at issue sustained an outage. Additionally, the devices are non-critical Cyber Assets, and accordingly are afforded the protections of CIP-002 through CIP-009 applicable to non-critical Cyber Assets. Lastly, the undocumented switch was contained in the same Physical Security Perimeter (PSP).	NPCC_URE1 mitigated this issue by disconnecting the devices at issue and the undocumented switch and re-connecting it to switches that were documented. NPCC_URE1 reviewed the logs on the devices and found no evidence that there was any unauthorized access to the system via the undocumented switch.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012009847	CIP-005-1	R1.5	During an on-site Compliance Audit, NPCC discovered that NPCC_URE2 had an issue with CIP-005-1 R1.5. Specifically, four NPCC_URE2 Cyber Assets that control or monitor access to the Electronic Security Perimeter (ESP) were not running anti-virus and anti-malware tools, as required by CIP-007-1 R4. NPCC_URE2 failed to submit a timely Technical Feasibility Exception (TFE) request for the four devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE2 had existing compensating measures in place. Specifically, the Critical Cyber Assets (CCAs) within the ESP had mitigating measures in place to minimize the impact of a virus. Specifically, NPCC_URE2 utilizes a service contractor to monitor the ESP, and any intrusions or attempts to breach the ESP are immediately detected and reported to properly mitigate any risk. This is an open-ended TFE and the compensating measures have been in place since 2010.	This issue was mitigated through the TFE process. NPCC_URE2 filed the Part A TFE with NPCC. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012009849	CIP-007-1	R4	During an on-site Compliance Audit, NPCC discovered that NPCC_URE2 had an issue with CIP-007-1 R4. Specifically, three devices inside the Electronic Security Perimeter (ESP) were not running anti-virus and anti-malware tools, as required by the Standard. NPCC_URE2 failed to submit a timely Technical Feasibility Exception (TFE) request for the three Cyber Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE2 had existing compensating measures in place. Specifically, NPCC_URE2 had firewalls in place and the devices at issue did not have access to the Internet. These devices are all located within the NPCC_URE2 ESP. The devices are only connected through a VPN router. NPCC_URE2 utilizes a procedure that disables the VPN router when not needed to reduce the risk of intrusions. The VPN router is only enabled when updates are necessary. When the updates are completed, the VPN router is again disabled. This process is logged. This procedure was identified by the NPCC auditors as a Best Practice during the on-site CIP Audit. This is an open-ended TFE and the compensating measures have been in place since 2010.	This issue was mitigated through the TFE process. NPCC_URE2 filed the Part A TFE with NPCC. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012009850	CIP-007-1	R5	During an on-site Compliance Audit, NPCC discovered that NPCC_URE2 had an issue with CIP-007-1 R5. Specifically, three NPCC_URE2 devices inside the Electronic Security Perimeter (ESP) are not capable of technically enforcing strong passwords. NPCC_URE2 failed to submit a timely Technical Feasibility Exception (TFE) request for the three devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE2 had existing compensating measures in place. NPCC_URE2 utilizes a procedural control for passwords for the devices at issue. The administrator for these devices ensures that strong passwords are used and that the password is changed annually or whenever there is a change in authorized personnel. The administrator is the person who sets the shared password for these devices, and changes the password when required. This is an open-ended TFE and the compensating measures have been in place since 2009.	This issue was mitigated through the TFE process. NPCC_URE2 filed the Part A TFE with NPCC. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012010134	CIP-006-3a	R1; R1.1; R1.2	During an on-site Compliance Audit, NPCC discovered that NPCC_URE2 had an issue with CIP-006-3 R1. Specifically, NPCC_URE2's control room Physical Security Perimeter (PSP) had a dropped ceiling that did not have a solid wall extending up to the ceiling, as required by R1.1 and R1.2. NPCC_URE2 failed to submit a timely Technical Feasibility Exception (TFE) request for the PSP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the control room was manned 24 hours a day, seven days a week. The control room also has an alarm system, physical access system, cameras and defense in depth, meaning that there are several security systems that monitor the PSP. Additionally, any visitors are escorted and signed in and out per NPCC_URE2's cybersecurity policy. This is an open-ended TFE and the compensating measures have been in place since 2009.	This issue was mitigated through the TFE process. NPCC_URE2 filed the Part A TFE with NPCC. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.

Attachment A-2

October 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012010135	CIP-006-3a	R2	During an on-site Compliance Audit, NPCC discovered that NPCC_URE2 had an issue with CIP-006-3 R2. Specifically, two NPCC_URE2 physical access control devices were not running anti-virus or anti-malware software, as required by CIP-007-3 R4.1. Specifically, certain parts of the devices do not support the installation of anti-virus software, as they do not contain an operating system with this capability. NPCC_URE2 failed to submit a timely Technical Feasibility Exception (TFE) request for the two devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the physical security systems at issue are not used to monitor or control Critical Cyber Assets and would have no impact on NPCC_URE2's Critical Cyber Assets if compromised. NPCC_URE2's Cyber Assets that authorize or log access to Physical Security Perimeters (PSPs) are afforded the protections specified in CIP-006-3a R2, with the exception of the parts of the devices described herein. These parts are located within the PSP. This is an open-ended TFE and the compensating measures have been in place since 2009.	This issue was mitigated through the TFE process. NPCC_URE2 filed the Part A TFE. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (RFC_URE1) Public Service Electric & Gas Company (PSE&G)	NCRXXXXX	RFC2012010440	CIP-006-3c	R8	During a Compliance Audit, ReliabilityFirst discovered that RFC_URE1 had an issue with CIP-006-3c R8. RFC_URE1 produced an inspection report stating that it must replace a door contact pursuant to its maintenance and testing program for physical security systems. The contractor who could fix the door was onsite at RFC_URE1 that day, so RFC_URE1 requested the contractor to repair the door. As a result, RFC_URE1 repaired the door the same day it discovered the issue. RFC_URE1, however, did not create a formal work order for the repair, and therefore failed to retain the record for the maintenance, as required by CIP-006-3c R8.2.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated because RFC_URE1 repaired the door contact the same day it discovered the issue and had just failed to document the maintenance work. The CIP-006 R8 issue discovered during the Audit began nine days prior to the discovery date. The problem with the door was that a contact was misaligned. The misaligned contact did not affect the magnetic lock on the door, so there was never unimpeded access. The door would only operate when an authorized individual swiped a badge. The bad contact only affected the transmission of the status of the door (“open” or “closed”) to the central monitoring system. The door in question is on a specific floor of RFC_URE1’s corporate headquarters. In order to access that door, there are two other sets of security protections. In order to gain unescorted access to the corporate headquarters an individual must pass through one of four turnstiles which are opened using a corporate ID card. Visitors must be escorted in order to gain access. Additionally, access to the entire floor is restricted by sliding glass doors on either end of the elevator bank access corridor. The remainder of the floor is only accessible to employees who have associated access privileges. Visitors must call someone and be met at one of the doors to gain access to the floor. The door in question resides behind both of these physical protections.	RFC_URE1 reinforced the requirement of documenting maintenance, with appropriate personnel including minor repairs completed when a technician is already on-site for other work. In addition, RFC_URE1 revised its maintenance and testing form to include two additional categories: "Follow Up/Date" and "Service Ticket Number" to document the work performed. Furthermore, RFC_URE1 now includes invoices documenting repairs in the maintenance and testing form.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012010434	CIP-005-3a	R5	RFC_URE2 self-reported an issue with CIP-005-3a R5 to ReliabilityFirst. Typically, RFC_URE2’s electronic access logs are automatically transferred daily from routers to a central log repository. Two issues occurred that prevented logging from these routers. First, the routers ran out of virtual memory which caused subsequent log records to overwrite previous log records. Second, the vendor’s technical issue prevented the automatic backup and storage of the logs on the central log repository. As a result, a portion of the log data that includes logging for attempts at or actual unauthorized access for these routers were not captured in the central log repository for over four months. RFC_URE2 began employing an alternate source on for one router and, 22 days later, for the remaining two routers, which successfully captured and retained logs for these three routers. As a result, there was a net loss of logs of 55 days for two routers and 35 days for the remaining router.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because the logging issue did not affect alerting for attempts at or actual unauthorized access as RFC_URE2's system issues alerts in real time. These alerts do not rely on the storage of log files in the central log repository. In addition, RFC_URE2 subsequently retrieved and retained log files resulting in the recovery of log files for one router and 22 days later for the other two routers.	RFC_URE2 committed to take certain actions to mitigate the issue. RFC_URE2 implemented an alternate logging source, which began capturing and retaining logs. In addition, RFC_URE2 ensured that the vendor resolved the technical issue on the centralized log repository.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012009866	CIP-004-3	R4	RFC_URE3 self-reported an issue with CIP-004-3 R4. A RFC_URE3 contract security officer resigned from the RFC_URE3 contractor. RFC_URE3 previously granted the contract security officer authorized unescorted physical access to areas containing Critical Cyber Assets (CCAs). RFC_URE3, however, failed to update its list of personnel who have physical access to (CCAs) until about 5 months after the contract security officer resigned which was not within seven calendar days of this change in access rights of personnel, as required by CIP-004-3 R4.1. In addition, RFC_URE3 failed to disable the contract security officer’s physical access badge within seven calendar days, as required by CIP-004-3 R4.2. RFC_URE3 disabled the contract security officer’s physical access badge; however, the contract security officer still had the physical access badge when RFC_URE3 discovered the issue. 15 days after RFC_URE3 disabled the physical access badge, the contract security officer voluntarily surrendered the badge.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system because prior to the time period of the issue, the contract security officer had cybersecurity training and a valid personnel risk assessment, which included an extensive background check similar to that required for unescorted access to nuclear power plants, a driving record review and stringent fitness for duty testing. In addition, the contract security officer never had authorized cyber access to CCAs, and operations personnel occupy the areas to which the contract security officer had access 24 hours a day. As a result of the foregoing, it was less likely that the contract security officer could gain access unnoticed and cause harm to the integrity of the CCAs. Furthermore, the contract security officer did not physically access the areas containing CCAs during the time period of the issue.	RFC_URE3 committed to take certain actions to mitigate the issue. RFC_URE3 disabled the contract security officer’s physical access badge. In addition, RFC_URE3 established an internal process whereby the security contractor will communicate employee status changes to appropriate RFC_URE3 management personnel regarding security personnel that is distinct from the pre-existing weekly roster updates. Furthermore, the security contractor will follow up within 24 hours of that out-of-service effective date to verify that RFC_URE3 has removed access within 24 hours. If RFC_URE3 has not removed access, the system will send a second notification. In addition, RFC_URE3 began generating weekly automated emails that provide to its contractors and vendors lists of its employees who have authorized unescorted physical access to CCAs. The contractors and vendors are directed to review the lists to determine whether access is still required and to reply whether any require cancellation. If there is no reply during the same week, RFC_URE3 will cancel access for those individuals.

Attachment A-2

October 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP2012009705	CIP-007-1	R5.3	SPP RE_URE1 submitted two Self-Reports to SPP RE stating that it was noncompliant with CIP-007-1 R5.3.2 and R5.3.3. Because CIP-007-1 R5.3.2 and R5.3.3 are closely related, SPP RE consolidated the two Self-Reports into one Self-Report. Regarding R5.3.2, SPP RE_URE1 reported that during an internal compliance audit, SPP RE_URE1 identified 23 accounts with access to its Energy Management System (EMS) that had passwords that did not consist of a combination of the three required character types (alpha, numeric and "special" characters). The passwords did consist of at least seven characters, and contained alpha and numeric characters, but failed to include a "special" character, as prescribed by R5.3.2. Regarding R5.3.3, SPP RE_URE1 identified three devices that had not had their passwords changed annually.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE1 had accounts that did not fully conform to the CIP-007-1 R5.3.2 requirement, these accounts did conform to two out of the three criteria listed in the subrequirement. Furthermore, all of the accounts that were not compliant with CIP-007-1 R5.3 were under continuous monitoring via an automated event and monitoring solution that provided unauthorized access detection. There were no incidents or events of unauthorized access detected during SPP RE_URE1's period of noncompliance.	SPP RE_URE1 changed passwords on its EMS Critical Cyber Assets (CCAs), Protected Cyber Assets (PCAs), and electronic access control systems (EACSs) to meet the following requirements: 1) Length: Passwords shall be a minimum of 8 characters. 2) Complexity: Passwords shall consist of a combination of upper and lower alpha, numeric, and "special" characters. 3) Frequency: Passwords, at a minimum, shall be changed on an annual basis. SPP RE_URE1 also notified users of the requirement to select and use passwords that meet the complexity requirements as detailed in its passwords requirement document. Finally, SPP RE_URE1 changed passwords on every EMS CCA, PCA and EACS to comply with the CIP-007-1 R5.3 Requirements.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP2012009924	CIP-004-1	R4.1	During a CIP Compliance Audit of SPP RE_URE2, the SPP RE CIP Audit Team identified noncompliance with CIP-004-1 R4.1 related to the quarterly reviews of SPP RE_URE2's list of personnel with access to Critical Cyber Assets (CCAs). Specifically, the audit team determined that SPP RE_URE2 could not demonstrate that it had reviewed its lists of personnel with electronic access to CCAs on a quarterly basis during the audit period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE2 could not show that it had reviewed the list of personnel with electronic access to CCAs quarterly, it did demonstrate that it reviewed the list of personnel with physical access to CCAs quarterly, as required by this Standard. Furthermore, SPP RE_URE2 demonstrated that it had conducted an annual review of access privileges, including electronic access, to CCA information, as required by CIP-003-3 R5. Finally, SPP RE_URE2 has a small number of employees with electronic access, and a low employee turn-over rate. Accordingly, changes to these employees' electronic access privileges would have been noticed by SPP RE_URE2 IT staff, despite the lack of a quarterly review.	SPP RE_URE2 conducted quarterly reviews of electronic access rights, transferring the responsibility to perform these reviews to the CIP compliance specialist, who is knowledgeable about electronic access rights. Additionally, SPP RE_URE2 updated its list to more efficiently identify those individuals with electronic access.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP2012009929	CIP-006-1	R1	During a CIP Compliance Audit of SPP RE_URE2, the SPP RE CIP Audit Team identified SPP RE_URE2's noncompliance with CIP-006-1 R1. A SPP RE_URE2 employee inappropriately gave itself physical access to a Physical Security Perimeter (PSP), the control room (SPP RE_URE2's backup control center), without following the procedures established in the SPP RE_URE2 Physical Security Plan. SPP RE_URE2's Physical Security Plan requires employees to get permission from the appropriate manager or supervisor and to complete the authorized access procedures before being granted access. The employee accessed the control room PSP in order to perform testing of the security door contact. The PSP in which the employee granted itself access to was a recently re-designated PSP. The re-designation had split one PSP into two PSPs. The SPP RE_URE2 employee lacked permission to access the re-designated PSPs. However, prior to the re-designation, the SPP RE_URE2 employee did have access to the one PSP. The SPP RE_URE2 employee granted itself access at 12:23 p.m., and terminated access at 12:25 p.m., after testing the door devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although the SPP RE_URE2 employee inappropriately gave itself physical access to the control room, the employee had access to the control room prior to its re-designation from one PSP, to two PSPs. Additionally, records show that the employee's access to the control room existed only for a total of two minutes for the purpose of testing the doors. The employee had the necessary training and Personnel Risk Assessment (PRA).	SPP RE_URE2 took disciplinary action against the SPP RE_URE2 employee and counseled the employee on the correct process to follow to gain access to PSPs. SPP RE_URE2 granted the employee authorized access to the control room PSP.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP2012009931	CIP-006-1	R3	During an SPP RE CIP Compliance Audit of SPP RE_URE2, the SPP RE CIP Audit Team discovered a remediated issue of CIP-006-3 R5. The Audit Team observed that SPP RE_URE2 had not implemented technical controls for monitoring physical access at an access point between two Physical Security Perimeters (PSP), SPP RE_URE2's control room and SPP RE_URE2's computer room.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE2 did not have monitoring measures in place for the access point between its control room and computer room, the access point did have a keyed lock securing SPP RE_URE2's control room from any entry from the computer room. The keyed lock at the access point did not secure SPP RE_URE2 computer room from entry from the control room. Individuals with approved access to SPP RE_URE2's control room also have approved access to the computer room. Besides having a physical access control for the access point between the two PSPs, SPP RE_URE2 also had security measures in place at the access point to the building that housed the two PSPs. The building housing the PSPs has security guards, a barbed-wire fence surrounding the building, two steel doors, which were alarmed and a magnetically locked access door.	SPP RE_URE2 combined the two PSPs thereby negating the need to monitor the door connecting them.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP2012009932	CIP-006-3c	R6	During a CIP Compliance Audit of SPP RE_URE2, the SPP RE CIP Audit Team identified SPP RE_URE2's noncompliance with CIP-006-3c R6. Specifically, the Audit Team identified three instances in which SPP RE_URE2 did not adhere to its Physical Security Plan when logging the escorted physical access of three visitors to SPP RE_URE2's control room Physical Security Perimeter (PSP). This remediated issue involved one SPP RE_URE2 employee and two outside visitors. According to SPP RE_URE2's Physical Security Plan, visitors must fill out a visitor's log in order to gain access to certain areas within SPP RE_URE2's facilities. The visitor logs identify the name of the visitor, the entry/exit date and time, and the name of the accompanying SPP RE_URE2 escort. In one instance, a SPP RE_URE2 employee visitor failed to record the PSP exit time, and in the second instance SPP RE_URE2 failed to record the PSP exit time of one outside visitor as well as the PSP exit time and name of the SPP RE_URE2 escort for another outside visitor.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE2 did not follow its procedures by recording the times that the three individuals exited a SPP RE_URE2 PSP, all three individuals went through multiple layers of security to gain access to the PSP. The additional security measures included: a check-in with SPP RE_URE2 security, issuance of a visitor's badge, and escorted access to enter the PSP. Additionally, the one SPP RE_URE2 employee that failed to record the SPP RE_URE2 PSP exit time, had been in the SPP RE_URE2 control center before, and had appropriately and completely filled out the visitor logs during those times. None of the outside visitors had the capability to enter the PSP without an escort. Finally, SPP RE_URE2's control room is manned 24/7 and has 24-hour visual security monitoring.	SPP RE_URE2 circulated a company-wide e-mail to all personnel reminding them of the need to follow the company procedures related to logging physical access to the PSPs. Furthermore, SPP RE_URE2 held training for employees regarding the procedures for entering and leaving its PSPs.

Attachment A-2

October 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXXX	TRE201100242	CIP-005-1	R3.2	TRE_URE1 self-reported that it failed to submit a technical feasibility exception (TFE) on a device CIP-005-1 R3.2 requirements. The device is not a Critical Cyber Assets (CCA) nor is it essential to the operation of any Cyber Assets. Previously, TRE_URE1 had filed a TFE for this device but for a different Standard. Therefore, Texas RE determined that the device is not a new device that was overlooked. The oversight occurred when filling out the TFEs because TRE_URE1 failed to file a TFE for this Standard. The mitigating measures put in place in accordance with the previously filed TFE for this device served as a mitigating measure during the period of this issue.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the device is not a CCA nor is it essential to the operation of any Cyber Assets. Further, Texas RE determined that the risk was mitigated by the fact that during the pendency of this issue, there were no means to gain cyber access this device. Additionally, this device had been included in a previously filed TFE and all mitigating measures put in place in accordance with the previous TFE were also in place during the pendency of this issue. Furthermore, the device is always protected by the surrounding protective systems on the PSPs and ESPs. This device is inside an Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP).	Because the device was covered by a previous TFE, the mitigation measures put in place for the previous TFE also serve to mitigate the risk of this instance of noncompliance.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXXX	TRE201100269	CIP-005-1	R3.2	TRE_URE1 self-reported that it failed to submit a technical feasibility exception (TFE) on a device. The device is not a Critical Cyber Assets (CCA) nor is it essential to the operation of any Cyber Assets. Previously, TRE_URE1 had filed a TFE for this device but for a different Standard and Texas RE approved the TFE. Therefore, Texas RE determined that the device is not a new device that was overlooked. The oversight occurred when filling out the TFEs because TRE_URE1 failed to file a TFE for this Standard. The mitigating measures put in place in accordance with the previously filed TFE for this device served as a mitigating measure during the period of this issue.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the device is not a CCA nor is it essential to the operation of any Cyber Assets. Further, Texas RE determined that the risk was mitigated by the fact that during the pendency of this issue, there were no means to gain cyber access this device. Additionally, this device had been included in a previously filed TFE and all mitigating measures put in place in accordance with the previous TFE were also in place during the pendency of this issue. Furthermore, the device is always protected by the surrounding protective systems on the PSPs and ESPs. This device is inside an ESP and PSP.	Because the device was covered by a previous TFE, the mitigation measures put in place for the previous TFE also serve to mitigate the risk of this instance of noncompliance.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXXX	TRE2012009765	CIP-004-2	R2	During an Audit it was discovered that TRE_URE1 did not update its cyber security training program at least annually. TRE_URE1's annual training stated that updating of its cyber security incident response plan as per CIP 008-1 R1.4 is required within ninety calendar days of any changes made. However, when Version 2 of the CIP Standards became effective on April 1, 2010, TRE_URE1 failed to update its annual training materials that reference CIP 008-1 R1.4. TRE_URE1 failed to provide a reference to the new Version of the Standard- CIP-008-2 R1.4, which requires any changes to be made within thirty calendar days instead of 90 calendar days. As a result, TRE_URE1 included incorrect information into its training materials. This issue existed from April 1, 2010 to January 11, 2012. Furthermore, Texas RE found an additional remediated issue during the Compliance Audit. Seven TRE_URE1 contractors with access to Critical Cyber Assets (CCAs) were not trained as required by CIP-004-2 R2.3. However, TRE_URE1 failed to train them by that date and did not revoke their access until four days after training should have been completed. As a result, Texas RE determined that TRE_URE1 had a remediated issue with CIP-004-2 R2.3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although TRE_URE1 employees were being trained with training material that did not fully reflect a change in the Reliability Standards Versions, the employees received a timely training on all other aspects of the Standard. Also, all trained employees at issue had Personnel Risk Assessment (PRAs) performed and were knowledgeable about TRE_URE1's CCAs' security practices. For sub requirements R2.3, the contractors having access to these CCAs had previously had cyber security training, and their PRAs were current. Therefore, Texas RE determined that these contractors were familiar with TRE_URE1's security practices. Finally, TRE_URE1 was noncompliant with R2.3 for a period of four days, which reduced the risk to the BPS to minimal.	To mitigate this issue TRE_URE1 has provided an updated training program document, which reflects the change from Version 1 to Version 2 of this CIP Standard. TRE_URE1 also trained the contractors at issue.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXXX	TRE2012009766	CIP-002-1	R3	During a Compliance Audit Texas RE discovered that TRE_URE1 did not develop a list of Critical Cyber Assets (CCAs) using the list of Critical Assets determined through an application of TRE_URE1's risk-based assessment methodology (RBAM). Specifically, Texas RE determined that one device was incorrectly excluded from the list of CCAs because TRE_URE1 failed to follow its RBAM for developing a list of CCAs. An inaccurate filtering criteria was assigned to the device that caused it to be marked as not being a CCA. However, TRE_URE1 was aware that the device was a CCA and afforded all the security measures required by the Reliability Standards to it. No other instances of incorrect filtering were discovered during the Compliance Audit.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The CCA at issue was located inside a Physical Security Perimeter (PSP), was monitored by an electronic entrance, and was firewalled. In addition, the CCA was subject to staff oversight at TRE_URE1's Electronic Security Perimeters (ESPs) and the PSP, and it was accessible only to designated staff members with Personnel Risk Assessments (PRAs). Documents show that the CCA at issue was considered as part of the CCA list. The security of the CCA was not compromised during the three-month period of- TRE_URE1's noncompliance.	To mitigate this issue TRE_URE1 has provided a CCA list document, showing that marketing PC1 been documented as a CCA. The document was signed by the Senior Manager.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXXX	TRE2012009773	CIP-008-2	R1.4	During a Compliance Audit, Texas RE discovered that TRE_URE1's Cyber Security Incident response plan (Versions 2009 and 2011) stated that changes to the plan are to be incorporated into the plan within 90 days, not within 30 days, as required by Version 2 of this Standard -CIP-008-2 R1.4. Version 1 of this Standard required that any change be incorporated within 90 days.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE determined that this remediated issue is documentation- related and administrative in nature because there were no changes to the plan during the period of noncompliance. Further, any changes to the plan would still have been incorporated within 90 days, thereby further reducing the risk to the BPS.	TRE_URE1 updated its Cyber Security Incident response plan, which is part of its training program, to require that any changes are incorporated within 30 days.

Attachment A-2

October 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201100155	CIP-006-1	R1.8	TRE_URE2 self-reported noncompliance with CIP-006-1 R1.8. As part of the annual cyber vulnerability assessment (CVA), TRE_URE2 identified noncompliance. Texas RE determined that the system was not afforded the protective measured required by this Standards, a process to grant access was not used, not all accounts have been changed because the vendor has indicated that there may be negative impacts, the documented process for granting access to the device and associated hardware was not used to grant access, shared accounts that did not meet the password complexity and annual change frequency requirement, physical security monitoring alarm processes were not correctly followed by one employee per documented procedures, the devices were configured to enable all users with a network account to log on locally, employees were given system access to the badging servers prior to completion of background check, and responsibility for patch management for the badging servers was not defined or automated, and patches were not installed.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). TRE_URE2 badging servers are completely separate from TRE_URE2's Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). Exposure was limited by the fact that the devices were in Physical Security Perimeters (PSPs) with controlled access, essentially limiting access to only people with the appropriate Personnel Risk Assessment (PRAs). Texas RE determined that in the worst case scenario would result in TRE_URE2 PSP doors unlocking. Even if this occurred, TRE_URE2 facilities are protected 24/7. Also, the device quadruple (4X) is redundant. TRE_URE2's assessed the other security layers and determined that no actual intrusion or criminal activity occurred as a result of this failure to follow procedure. The servers had up to date monitored antivirus.	TRE_URE2 stated that the following mitigation activities have been completed: 1) CIP-005-3 R2: This was corrected and validated by TRE_URE2's gap analysis team. Access authorization documentation and procedures have been reviewed. 2) CIP-007-3 R5.1: Local logon service has been reduced to allow only personnel with a business need to logon to the system. 3) CIP-007-3 R3: device was updated with current security patches and verified by a vulnerability assessment scanning tool. Responsibility for patch installation has been clearly defined. 4) CIP-007-3 R5, R5.2, R5.3: The process has been documented and implemented. As a future improvement, all access control and verification will be performed with a single access control tool. Not all of the accounts have been changed because the vendor has indicated that there may be negative impacts. TRE_URE2 worked with the vendor to resolve this issue. 5) CIP-006-3 R5: The employee received corrective training to ensure documented procedures will be followed, along with monitoring of compliance for this specific physical security monitoring function.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201100400	CIP-005-1	R1.5	TRE_URE2 self-reported noncompliance with CIP-005-1 R1.5 for a failure to afford the protective measures specified in Standards CIP-007 R1 and R3 through R9. TRE_URE2 utilizes several applications and servers to administer firewalls, to provide logs, and to produce email alerts and reports for malicious activities for its Electronic Security Perimeter (ESP). As part of the CIP gap analysis, TRE_URE2 identified and self-reported noncompliance with CIP-005-1 R1.5 because it failed to afford all of the protective measures required by this Standard for two applications and two servers. The servers are physically located inside the PSP, but outside the Electronic Security Perimeter (ESP). For an application, TRE_URE2 failed to implement an acceptable use banner on one instance, the application did not log user activity, server access was not reviewed on annual basis, and three shared accounts did not identify and document individual users for the servers. For another application, TRE_URE2 identified three shared accounts with default passwords that allow access, and two of the accounts did not meet the password complexity requirement. TRE_URE2 failed to implement a patch management process for other servers.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1) Remote access to the servers at issue is limited. The default account can only be accessed locally, within a protected physical area. Individuals that can logon to the microcontrollers have a current and valid Personnel Risk Assessment (PRA) and cyber security training. Interactive login was limited to specific workstations with static IP addresses. These workstations were assigned to employees who already had authorized access, and who had PRAs and had completed cyber security training. 2) The systems at issue are not directly accessible from the Internet, reside in a PSP with limited access, are physically and electronically segregated from TRE_URE2's Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS), and run anti-virus scans. No virus detections have occurred during the pendency of this remediated issue.	TRE_URE2 completed all mitigating activities related to this issue, including the following measures: 1) Acceptable use banners on the application and servers were installed; 2) Logging capability for the application and servers were enabled; 3) TRE_URE2 expanded its existing cyber security procedures; 4) The passwords complexities were identified on the accounts at issue; and 5) System patches and security updates were completed and verified by a vulnerability assessment scan.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE2012009733	CIP-007-1	R5.2	TRE_URE2 self-reported an issue with CIP-007-1 R5.2 for a failure to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factor default accounts. TRE_URE2 utilizes its Energy Management System (EMS) to monitor and control its Transmission Operator (TOP) area. The EMS has been identified as a Critical Cyber Asset (CCA) per TRE_URE2's methodology. As part of its CIP gap analysis, TRE_URE2 self-reported noncompliance with CIP-007-1 R5.2. For three shared accounts, TRE_URE2 could not demonstrate compliance, as specified in Requirement 5, with the documentation procedures required by its account management program. The policy requires identification of all computers with shared accounts. In addition, TRE_URE2 could not identify those individuals with access to one of the three shared accounts.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1) The EMS system is located within the Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP). The system is only accessible to personnel with approved unescorted access to the Critical Cyber Asset. 2) TRE_URE2 demonstrated its password policy was compliant with the requirements of CIP-007-1 R5.3. TRE_URE2 implemented its policy for all three shared accounts .	The following mitigation activities have been completed: TRE_URE2 documented the computers with shared access implementing their policy to minimize and manage the use of shared account privileges.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3) CPS Energy (CPS)	NCRXXXXX	TRE2012010289	CIP-003-1	R1.1	During a Compliance Audit Texas RE found that TRE_URE3 was noncompliant with CIP-003-1 R1 because its cyber security policy failed to address the requirements in Standards CIP-002 through CIP-009. Texas RE determined that TRE_URE3 2009 and 2010 versions of its cyber security policy did not address the requirements in Standards CIP-002 through CIP-009, but its 2011 Version did address these Requirements. Specifically, TRE_URE3's policy presented failed to adequately address the following two requirements: CIP-007-2 R5 and CIP-003-2 R5.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). TRE_URE3 was able to provide documentation on all other aspects of their NERC Cyber Security Policy document for 2010 and 2009 and the updated version for 2011 addressed the requirements of this Standard. Texas RE determined that the risk was mitigated by the fact that TRE_URE3 had a policy prior to the mandatory compliance date. TRE_URE3's Cyber Security Plan has been in place for years, annually reviewed, updated according to CPS' internal document control procedures, and adequately addressed the vast majority of the requirements in Standards CIP-002-2 thorough CIP-009-2. TRE_URE3's policies did not contain low-level, specific details and requirements related to the implementation of the policy. However, these details were contained in other processes and procedures that supported compliance with the security policy	The updated policy addresses each applicable CIP standard and requirement. Under each requirement there is a brief description of how TRE_URE3 meets that requirement. The updated policy mitigates this remediated issue.

Attachment A-2

October 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012010304	CIP-007-1	R4	WECC_URE1, as a Balancing Authority, Generator Operator, Generator Owner, Load Serving Entity, Transmission Operator, Transmission Owner, and Transmission Service Provider, self-reported an issue with of CIP-007-1 R4. A WECC Subject Matter Expert (SME) contacted WECC_URE1 to discuss its Self-Report. According to the WECC SME, WECC_URE1 stated that for five devices it failed to use anti-virus software and other malicious software prevention tools. WECC_URE1 also stated that it is technically infeasible to use anti-virus or anti-malware software on these devices and intended to file a Technical Feasibility Exception (TFE). The WECC SME concluded that WECC_URE1 had an issue with CIP-007-1 R4 and referred the matter to Enforcement. Enforcement determined that WECC_URE1 had an issue with CIP-007-1 R4 because it neither installed anti-virus or anti-malware software on the CCAs described above, nor did WECC_URE1 file TFEs for the devices involved.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because The CCAs are devices used as a communication link for managing serially connected devices. As compensating measures, the devices are located in an Electronic Security Perimeter and have technical and procedural mechanisms for control of electronic access at all access points. WECC_URE1 enabled only those ports and services necessary at the access points and required username and passwords to access the devices. Also, all devices are located within a Physical Security Perimeter with procedural controls to manage physical access, including 24/7 logging and monitoring of physical access. Additionally, if the devices were to lose connectivity, alarms alert staff. WECC_URE1 filed TFEs for the devices because it was technically infeasible to install anti-virus and anti-malware software on the devices. WECC approved the TFEs.	WECC_URE1 completed mitigation of this issue.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010965	CIP-006-3c	R2.2	WECC_URE2, as a Balancing Authority, Generator Operator, Load Serving Entity, Transmission Operator, Transmission Owner, and Transmission Service Provider, self-reported an issue with CIP-006-3c R2.2. WECC_URE2 reported that it failed to file Technical Feasibility Exceptions (TFE) for two Critical Cyber Assets (CCAs) that authorize and/or log physical access to a Physical Security Perimeter (PSP). WECC Subject Matter Experts (SMEs) reviewed WECC_URE2's Self-Report and TFE requests. SMEs determined it is technically infeasible for WECC_URE2 to install anti-virus software on the two devices. WECC Enforcement reviewed WECC_URE2's Self-Report, the SMEs' findings, and TFE approvals and determined that WECC_URE2 failed to submit a TFE as required under CIP-007-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because WECC_URE2 had compensating measures in place to secure the devices against misuse or malicious attack. CIP-006-3 R2.2 requires entities to afford these devices protections specified in twenty-four Standard Requirements. In this case, WECC_URE2 failed to afford two devices one protection specified in CIP-007-3 R4. Specifically,-WECC_URE2 failed to file TFEs for two devices on which it was technically infeasible to implement anti-virus software. WECC_URE2 secured both devices within an Electronic Security Perimeter (ESP). Electronic access was logged and monitored. Individuals with electronic access completed Personnel Risk Assessments (PRAs) and cyber security training. WECC_URE2 controlled access to the ESP with restricted user accounts, passwords, intrusion detection, and alarms. WECC_URE2 installed alarms to alert personnel of unauthorized physical access to the Physical Security Perimeter. WECC_URE2 secured the devices within a facility to which access was controlled and monitored. Individuals with physical access to the devices completed PRAs. WECC_URE2 enabled only necessary ports and services on both devices.	WECC_URE2 completed mitigation of this issue.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3) Pend Oreille County Public Utility District No. 1 (POPD)	NCRXXXXX	WECC2012010468	CIP-002-3	R1	During a compliance audit WECC determined that WECC_URE3 had an issue with CIP-002-3 R1. WECC discovered that WECC_URE3 implemented a revised version of its risk-based assessment methodology (RBAM). Although the document contained procedures and evaluation criteria, it failed to contain a risk-based assessment component. The WECC Audit Team referred its finding to the WECC Enforcement (Enforcement). Enforcement reviewed the Audit Team's findings and determined that WECC_URE3 had an issue with CIP-002-3 R1, because it failed to identify and document an RBAM to identify its Critical Assets (CAs) and Critical Cyber Assets (CCAs).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because WECC_URE3 does not have CAs and does not have CCAs. As compensating measures, WECC_URE3's previous applications of its RBAMs generated null lists of CAs and CCAs. The WECC Audit Team determined that the existing null lists were accurate.	WECC_URE3 completed mitigation of the issue. WECC_URE3 proposed to revise its RBAM to document the risk-based component in detail. WECC_URE3 evaluated its Cyber Assets through an application of the updated RBAM to determine WECC_URE3's CAs. This process yielded a null set of Critical Assets for WECC_URE3.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012010763	CIP-003-1	R1	WECC_URE4 self-certified an issue with CIP-003-1 R1.3. A WECC Subject Matter Expert (SME) discussed with WECC_URE4 its self-certification. WECC_URE4 stated that it did not annually review its entire cyber security policy in the calendar year. Specifically, WECC_URE4 did not review cyber security policies that were outdated and not used by WECC_URE4. The WECC SME concluded that WECC_URE4 had an issue with CIP-003-1 R1.3 and referred the matter to WECC Enforcement. WECC Enforcement determined that WECC_URE4 had an issue with CIP-003-1 R1.3 because it did not perform a complete annual review of its cyber security policy for the calendar year.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the cyber security policies were outdated and not used by WECC_URE4. As compensating measures, WECC_URE4 stated that it did annual reviews and approved the current policies in use. WECC_URE4 did a full review of the cyber security policy in other calendar years.	WECC_URE4 completed mitigation of this issue. WECC_URE4 reviewed its cyber security policy in calendar year and removed the outdated items.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012010765	CIP-006-3c	R1	WECC_URE4 self-certified an issue with CIP-006-3c R1. A WECC SME contacted WECC_URE4 to discuss its self-certification. WECC_URE4 stated that one of its employees gained access to one of its Physical Security Perimeters (PSP) without having authorized access to the PSP. The employee involved accessed the PSP by walking through a door opened by another employee who had authorized access to the PSP. After the employee involved gained access to the PSP, alarms activated and the employee contacted WECC_URE4's security guards from a phone located next to the PSP door. Security instructed the employee to leave the PSP, which the employee did. The employee was inside the PSP for approximately one minute and did not access any Critical Cyber Assets (CCAs). The WECC SME concluded that WECC_URE4 had an issue with CIP-006-3c R1 and referred the matter to WECC Enforcement. WECC Enforcement reviewed the WECC SME's findings and the WECC_URE4 self-certification. Enforcement determined that WECC_URE4 had an issue with CIP-006-3c R1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the employees immediately contacted WECC_URE4's security guards and left the PSP without accessing any CCAs. As compensating measures, WECC_URE4 monitored the PSP 24 hours per day and each PSP access point has an alarm to alert of unauthorized physical access. In addition, WECC_URE4 staffs security at the facility 24/7. WECC_URE4's procedures for monitoring for unauthorized access proved effective as an alarm sounded, the employee immediately contacted WECC_URE4 security, and security instructed the employee to leave the PSP.	WECC_URE4 completed mitigation of this issue. WECC_URE4 remediated this issue when the employee who gained unauthorized access to the PSP left the PSP. WECC_URE4 trained personnel to instruct individuals who enter a WECC_URE4 PSP without an escort to immediately leave the PSP

Attachment A-2

October 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2012010361	CIP-004-3	R3	WECC_URE5 self-reported a an issue with CIP-004-3 R3. According to the Self-Report, one of WECC_URE5 employees had physical access to the a WECC_URE5 Physical Security Perimeter (PSP) for a period of 43 days after his personnel risk assessment (PRA) had expired. WECC determined that WECC_URE5 had an issue of CIP-004-3 R3 for failing to have an updated PRA for one of its employees.	WECC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because all Critical Cyber Assets (CCAs) reside within an identified PSP and Electronic Security Perimeter. Therefore, the CCAs were monitored and afforded the protections of CIP-005 and CIP-006. In addition, the employee involved had CIP-004 R2 training and is in good standing with WECC_URE5.	WECC_URE5 submitted a mitigation plan to address this issue. WECC approved the mitigation plan and certified its completion.

Document Accession #: 20121031-5394 **Filed Date: 10/31/2012**

Document Content(s)

FinalFiled_Oct_2012_FFT_20121031.PDF 1
FinalFiled_A-1(PUBLIC_Non-CIP_FFT)_20121031.XLSX 18
FinalFiled_A-2(PUBLIC_CIP_FFT)_20121031.XLSX.....26